This paper describes objective technical results and analysis. Any subjective views or opinions that might be expressed in the paper do not necessarily represent the views of the U.S. Department of Energy or the United States Government.

SAND2022-12709C

U.S. DEPARTMENT OF ENERGY | Office of Cybersecurity, Energy Security, and Emergency Response

Assessing Ransomware Activity in Operational Technology Environments Using Bayesian Networks

Gabriel Weaver and Lee Maccarone

2022 MORS Emerging Techniques Forum

Sandia National Laboratories is a multimission laboratory managed and operated by National Technology & Engineering Solutions of Sandia, LLC, a wholly owned subsidiary of Honeywell International Inc., for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-NA0003525.

Agenda

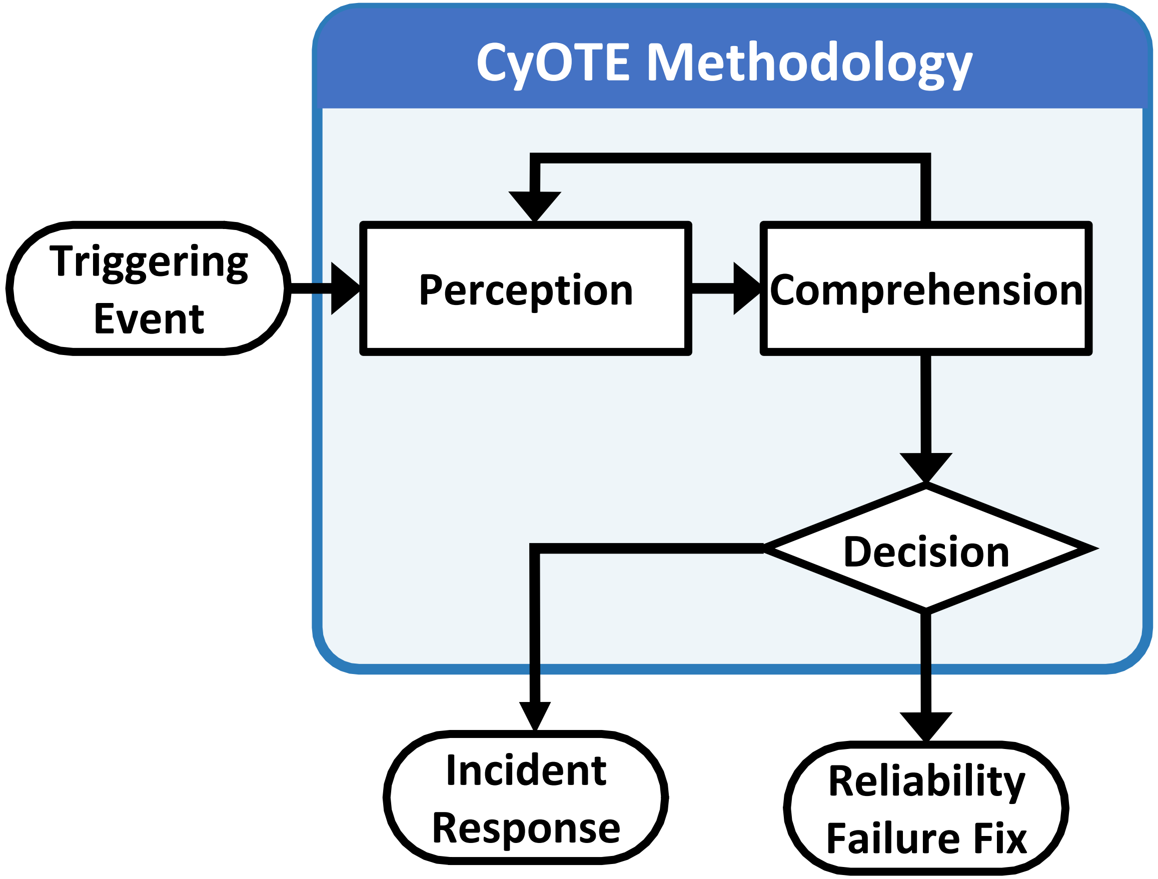
- Introduction to CyOTE
- Bayesian network overview
- EKANS case study
- Colonial Pipeline case study
- WannaCry case study
- Case study comparisons
- Take-aways

INL
Idaho National Laboratory

Sandia
National
Laboratories

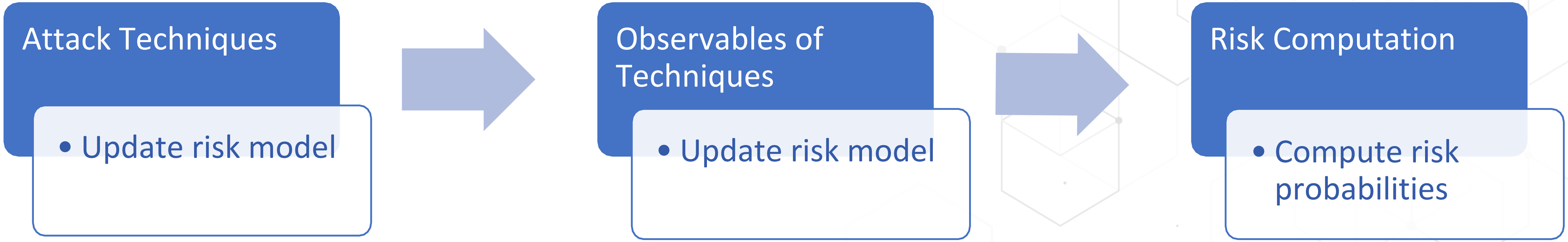
ITA
INTERNATIONAL

CyOTE Methodology Overview



- How to understand the information you have, not get more data
- Applies concepts of perception and comprehension to a world of Knowns and Unknowns
- Endpoint is making a risk-informed decision to conduct incident response or to treat as a reliability failure
- Over time, detect fainter signals sooner

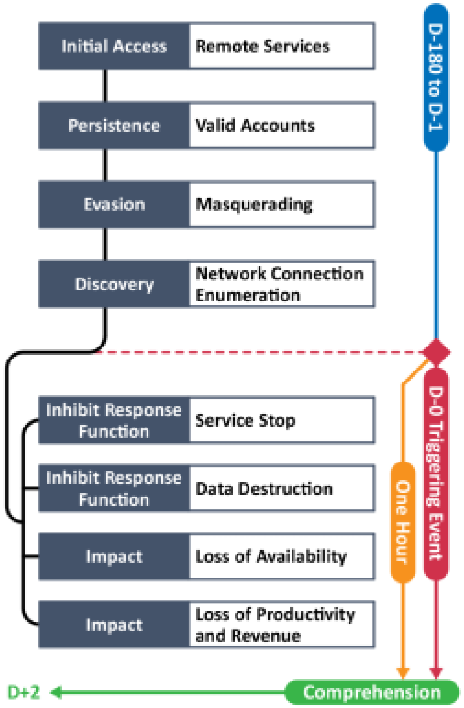
CyOTE Precursor Analysis Reports

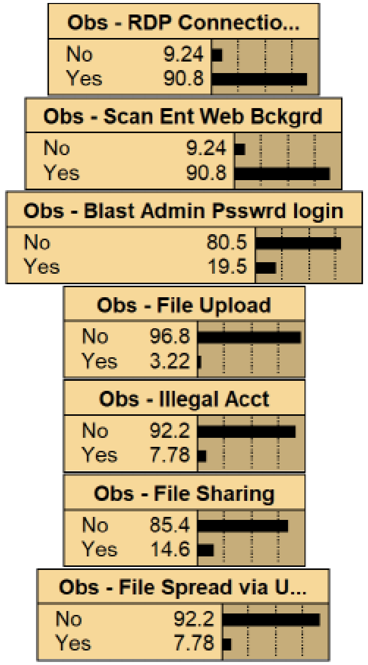


Attack Techniques
- Update risk model

Observables of Techniques
- Update risk model

Risk Computation
- Compute risk probabilities





Obs - RDP Connectio...	
No	9.24
Yes	90.8

Obs - Scan Ent Web Bckgrd	
No	9.24
Yes	90.8

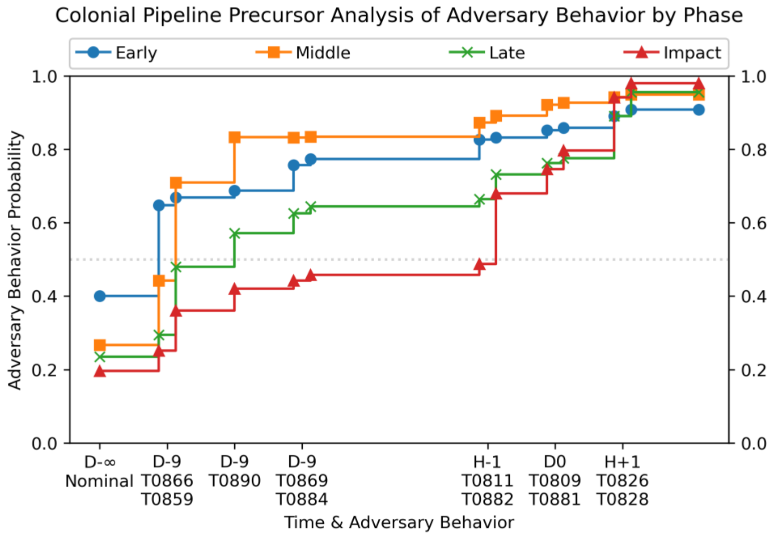
Obs - Blast Admin Psswrd login	
No	80.5
Yes	19.5

Obs - File Upload	
No	96.8
Yes	3.22

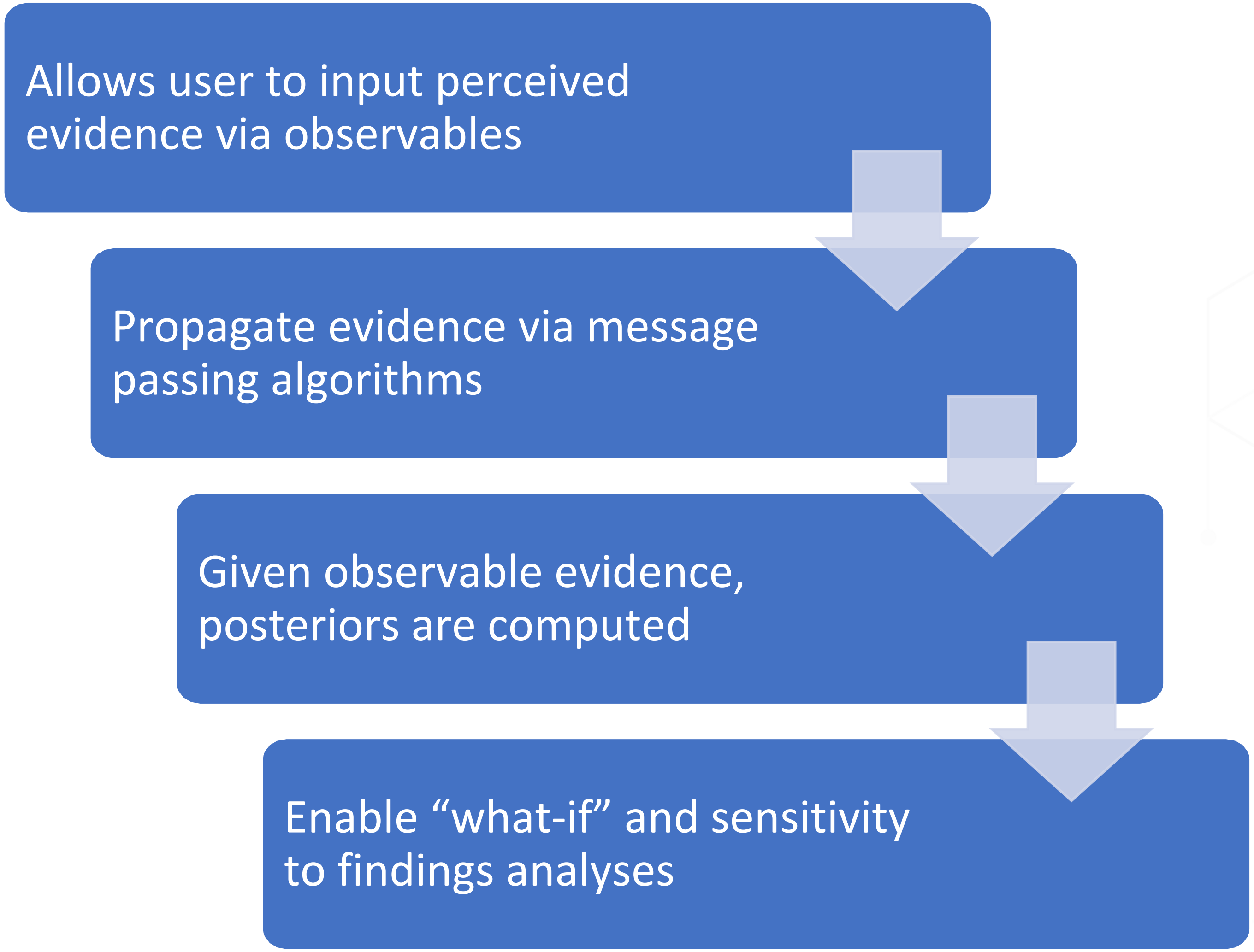
Obs - Illegal Acct	
No	92.2
Yes	7.78

Obs - File Sharing	
No	85.4
Yes	14.6

Obs - File Spread via U...	
No	92.2
Yes	7.78



Risk Approach: Bayesian Networks

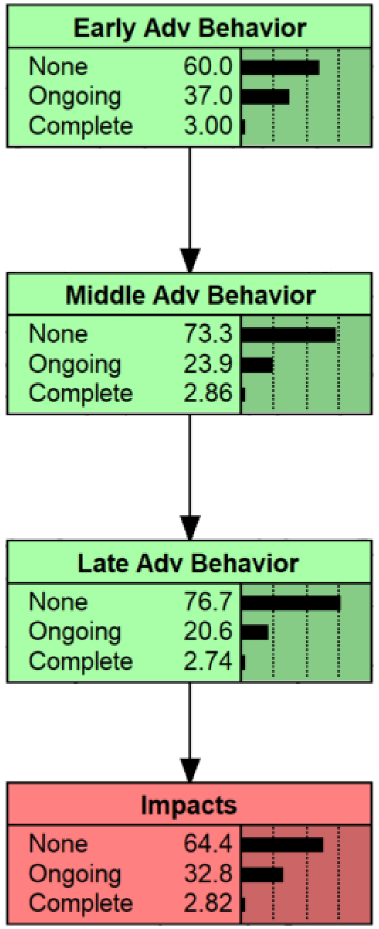


Allows user to input perceived evidence via observables

Propagate evidence via message passing algorithms

Given observable evidence, posteriors are computed

Enable “what-if” and sensitivity to findings analyses



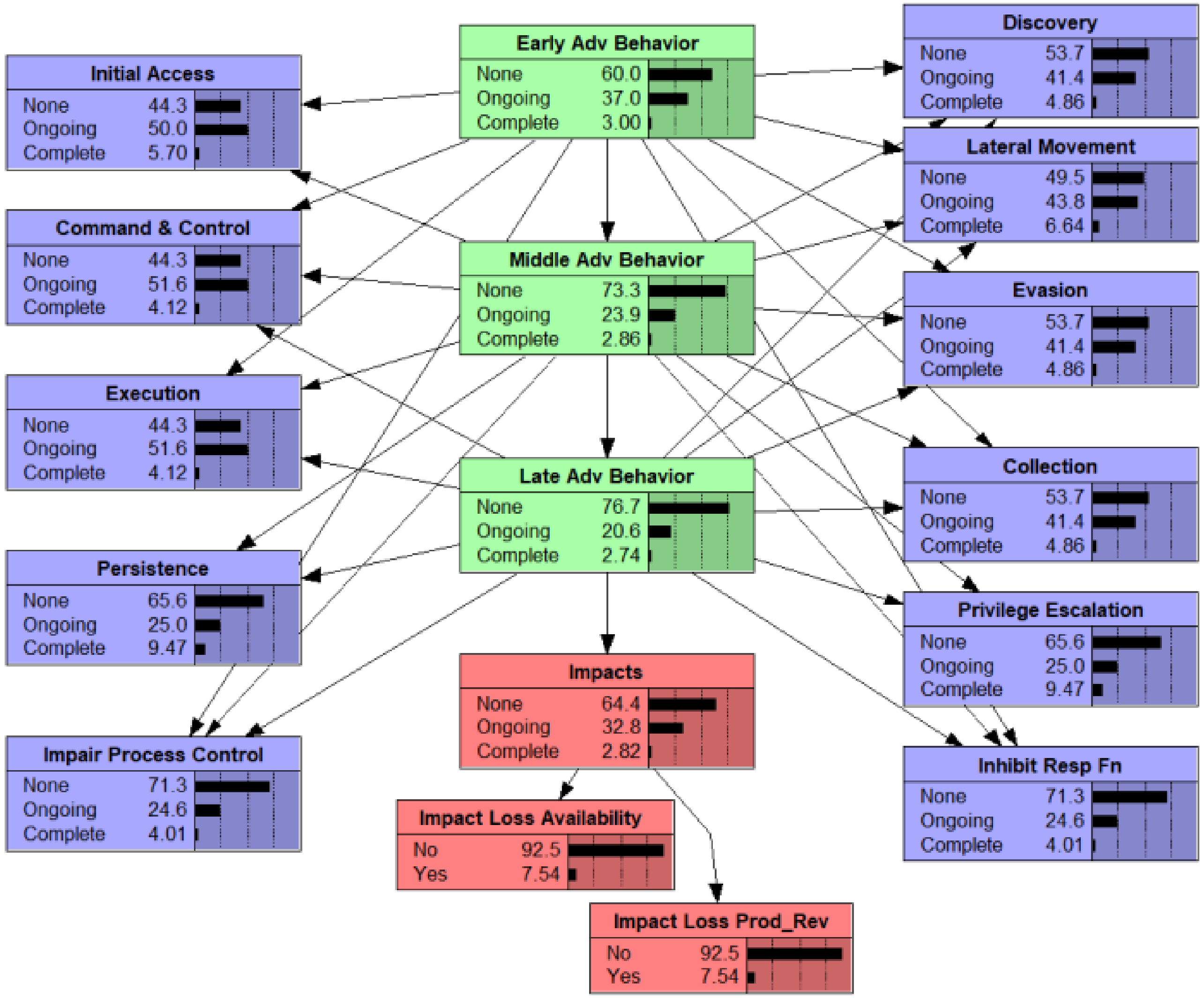
Core attack process

How is the network structured?

MITRE ATT&CK® for ICS

Initial Access	Execution	Persistence	Privilege Escalation	Evasion	Discovery	Lateral Movement	Collection	Command and Control	Inhibit Response Function	Impair Process Control	Impact
Drive-by Compromise	Change Operating Mode	Modify Program	Exploitation for Privilege Escalation	Change Operating Mode	Network Connection Enumeration	Default Credentials	Automated Collection	Commonly Used Port	Activate Firmware Update Mode	Brute Force I/O	Damage to Property
Exploit Public-Facing Application	Command-Line Interface	Module Firmware	Hooking	Exploitation for Evasion	Network Sniffing	Exploitation of Remote Services	Data from Information Repositories	Connection Proxy	Alarm Suppression	Modify Parameter	Denial of Control
Exploitation of Remote Services	Execution through API	Project File Infection		Indicator Removal on Host	Remote System Discovery	Lateral Tool Transfer	Detect Operating Mode	Standard Application Layer Protocol	Block Command Message	Module Firmware	Denial of View
External Remote Services	Graphical User Interface	System Firmware		Masquerading	Remote System Information Discovery	Program Download	I/O Image		Block Reporting Message	Spoof Reporting Message	Loss of Availability
Internet Accessible Device	Hooking	Valid Accounts		Rootkit	Wireless Sniffing	Remote Services	Man in the Middle		Block Serial COM	Unauthorized Command Message	Loss of Control
Remote Services	Modify Controller Tasking			Spoof Reporting Message		Valid Accounts	Monitor Process State		Data Destruction		Loss of Productivity and Revenue
Replication Through Removable Media	Native API						Point & Tag Identification		Denial of Service		Loss of Protection
Rogue Master	Scripting						Program Upload		Device Restart/Shutdown		Loss of Safety
Spearphishing Attachment	User Execution						Screen Capture		Manipulate I/O Image		Loss of View
Supply Chain Compromise							Wireless Sniffing		Modify Alarm Settings		Manipulation of Control
Transient Cyber Asset									Rootkit		Manipulation of View
Wireless Compromise									Service Stop		Theft of Operational Information
									System Firmware		

Tactics provide evidence for adversary behavior stage



Early Adv Behavior	
None	60.0
Ongoing	37.0
Complete	3.00

Middle Adv Behavior	
None	73.3
Ongoing	23.9
Complete	2.86

Late Adv Behavior	
None	76.7
Ongoing	20.6
Complete	2.74

Impacts	
None	64.4
Ongoing	32.8
Complete	2.82

Impact Loss Availability	
No	92.5
Yes	7.54

Impact Loss Prod_Rev	
No	92.5
Yes	7.54

Initial Access	
None	44.3
Ongoing	50.0
Complete	5.70

Command & Control	
None	44.3
Ongoing	51.6
Complete	4.12

Execution	
None	44.3
Ongoing	51.6
Complete	4.12

Persistence	
None	65.6
Ongoing	25.0
Complete	9.47

Impair Process Control	
None	71.3
Ongoing	24.6
Complete	4.01

Discovery	
None	53.7
Ongoing	41.4
Complete	4.86

Lateral Movement	
None	49.5
Ongoing	43.8
Complete	6.64

Evasion	
None	53.7
Ongoing	41.4
Complete	4.86

Collection	
None	53.7
Ongoing	41.4
Complete	4.86

Privilege Escalation	
None	65.6
Ongoing	25.0
Complete	9.47

Inhibit Resp Fn	
None	71.3
Ongoing	24.6
Complete	4.01

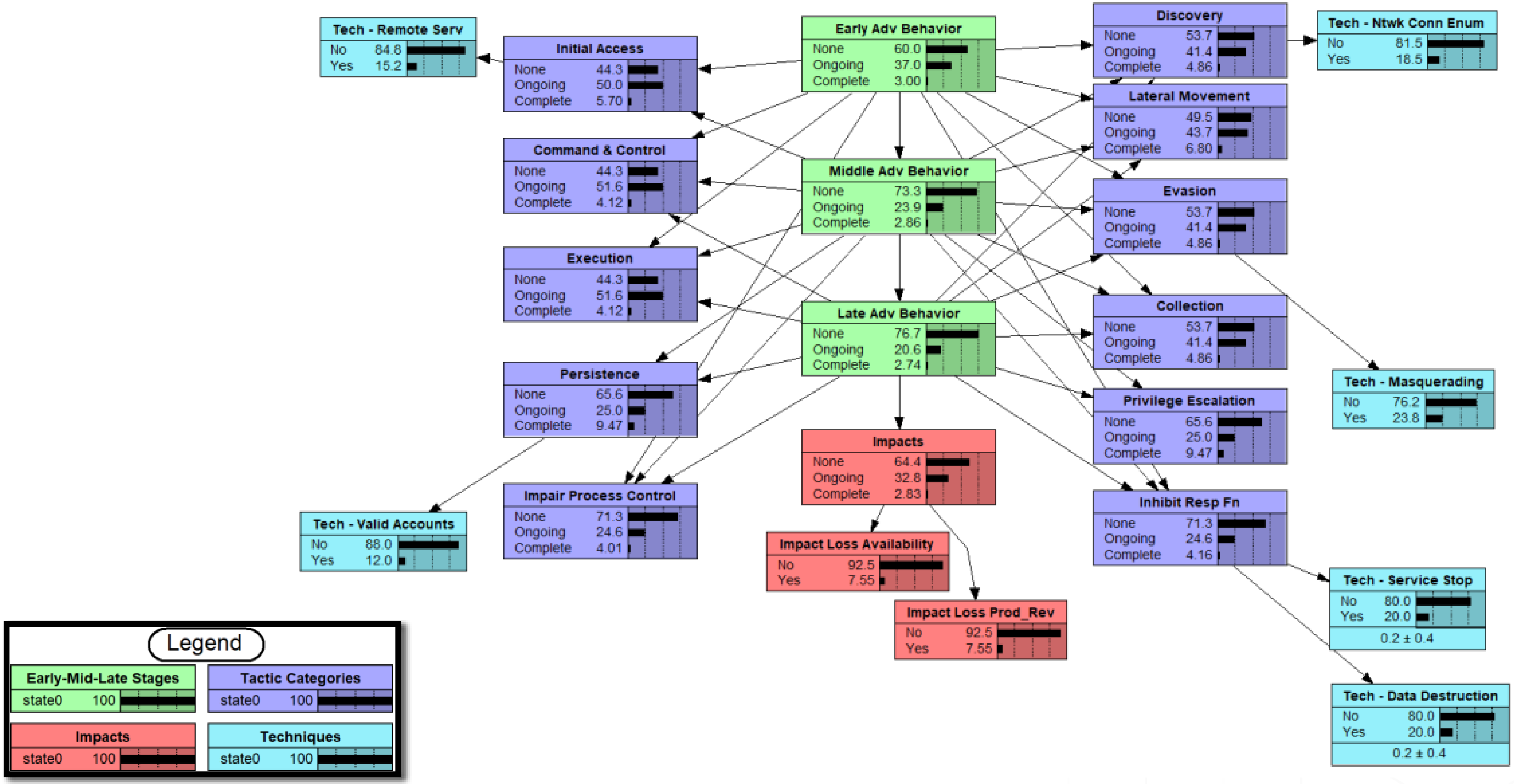
Legend

Early-Mid-Late Stages	
state0	100

Impacts	
state0	100

Tactic Categories	
state0	100

Techniques provide evidence for tactics



Tech - Remote Serv	
No	84.8
Yes	15.2

Initial Access	
None	44.3
Ongoing	50.0
Complete	5.70

Command & Control	
None	44.3
Ongoing	51.6
Complete	4.12

Execution	
None	44.3
Ongoing	51.6
Complete	4.12

Persistence	
None	65.6
Ongoing	25.0
Complete	9.47

Tech - Valid Accounts	
No	88.0
Yes	12.0

Impair Process Control	
None	71.3
Ongoing	24.6
Complete	4.01

Early Adv Behavior	
None	60.0
Ongoing	37.0
Complete	3.00

Middle Adv Behavior	
None	73.3
Ongoing	23.9
Complete	2.86

Late Adv Behavior	
None	76.7
Ongoing	20.6
Complete	2.74

Impacts	
None	64.4
Ongoing	32.8
Complete	2.83

Impact Loss Availability	
No	92.5
Yes	7.55

Impact Loss Prod_Rev	
No	92.5
Yes	7.55

Discovery	
None	53.7
Ongoing	41.4
Complete	4.86

Lateral Movement	
None	49.5
Ongoing	43.7
Complete	6.80

Evasion	
None	53.7
Ongoing	41.4
Complete	4.86

Collection	
None	53.7
Ongoing	41.4
Complete	4.86

Privilege Escalation	
None	65.6
Ongoing	25.0
Complete	9.47

Inhibit Resp Fn	
None	71.3
Ongoing	24.6
Complete	4.16

Tech - Ntwk Conn Enum	
No	81.5
Yes	18.5

Tech - Masquerading	
No	76.2
Yes	23.8

Tech - Service Stop	
No	80.0
Yes	20.0
0.2 ± 0.4	

Tech - Data Destruction	
No	80.0
Yes	20.0
0.2 ± 0.4	

Legend

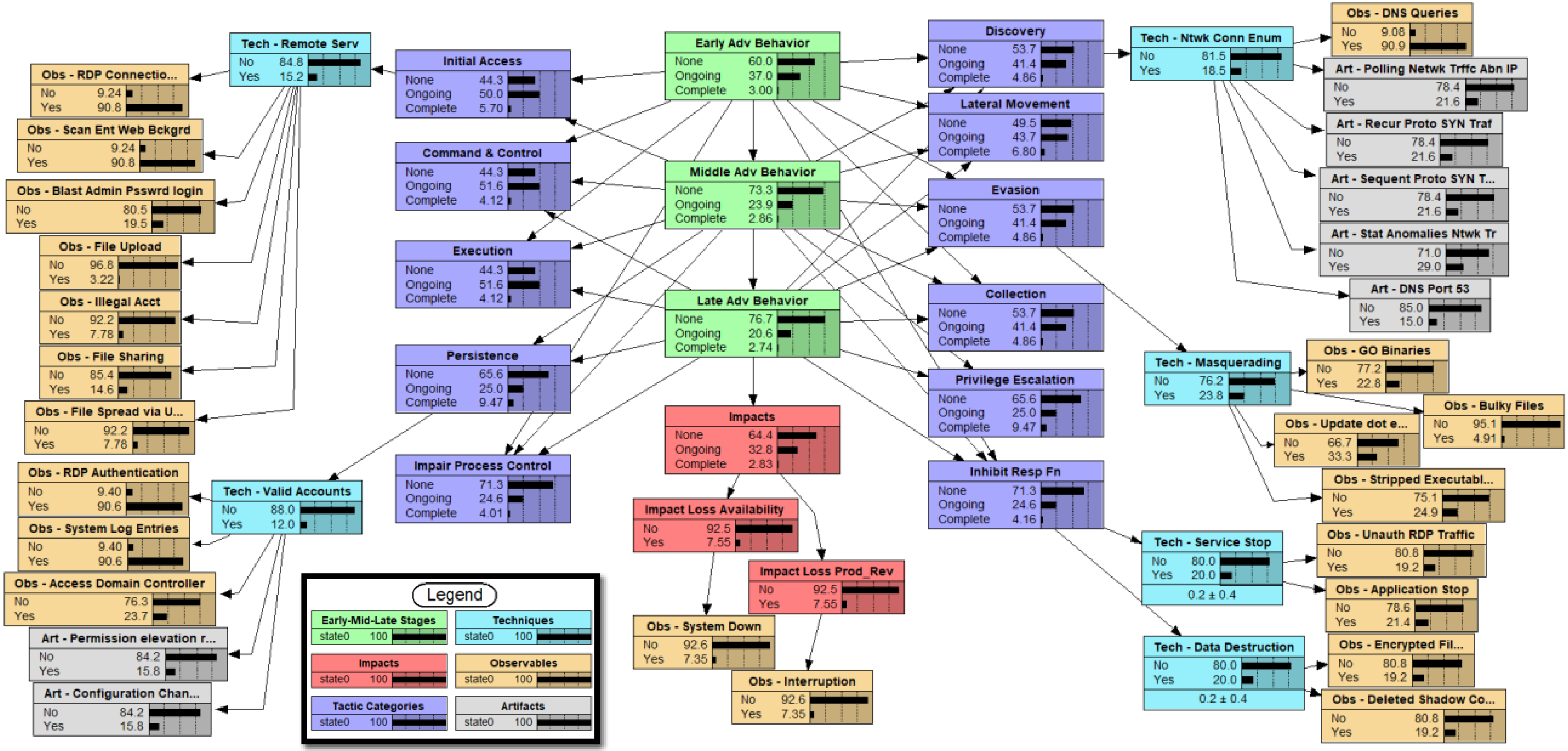
Early-Mid-Late Stages	
state0	100

Tactic Categories	
state0	100

Impacts	
state0	100

Techniques	
state0	100

Observables & artifacts provide evidence for techniques



Tech - Remote Serv
No 84.8
Yes 15.2

Obs - RDP Connectio...
No 9.24
Yes 90.8

Obs - Scan Ent Web Bckgrd
No 9.24
Yes 90.8

Obs - Blast Admin Psswrd login
No 80.5
Yes 19.5

Obs - File Upload
No 96.8
Yes 3.22

Obs - Illegal Acct
No 92.2
Yes 7.78

Obs - File Sharing
No 85.4
Yes 14.6

Obs - File Spread via U...
No 92.2
Yes 7.78

Obs - RDP Authentication
No 9.40
Yes 90.6

Tech - Valid Accounts
No 88.0
Yes 12.0

Obs - System Log Entries
No 9.40
Yes 90.6

Obs - Access Domain Controller
No 76.3
Yes 23.7

Art - Permission elevation r...
No 84.2
Yes 15.8

Art - Configuration Chan...
No 84.2
Yes 15.8

Initial Access
None 44.3
Ongoing 50.0
Complete 5.70

Command & Control
None 44.3
Ongoing 51.6
Complete 4.12

Execution
None 44.3
Ongoing 51.6
Complete 4.12

Persistence
None 65.6
Ongoing 25.0
Complete 9.47

Impair Process Control
None 71.3
Ongoing 24.6
Complete 4.01

Early Adv Behavior
None 60.0
Ongoing 37.0
Complete 3.00

Middle Adv Behavior
None 73.3
Ongoing 23.9
Complete 2.86

Late Adv Behavior
None 76.7
Ongoing 20.6
Complete 2.74

Impacts
None 64.4
Ongoing 32.8
Complete 2.83

Impact Loss Availability
No 92.5
Yes 7.55

Impact Loss Prod_Rev
No 92.5
Yes 7.55

Obs - System Down
No 92.6
Yes 7.35

Obs - Interruption
No 92.6
Yes 7.35

Discovery
None 53.7
Ongoing 41.4
Complete 4.86

Lateral Movement
None 49.5
Ongoing 43.7
Complete 6.80

Evasion
None 53.7
Ongoing 41.4
Complete 4.86

Collection
None 53.7
Ongoing 41.4
Complete 4.86

Privilege Escalation
None 65.6
Ongoing 25.0
Complete 9.47

Inhibit Resp Fn
None 71.3
Ongoing 24.6
Complete 4.16

Tech - Ntwk Conn Enum
No 81.5
Yes 18.5

Obs - DNS Queries
No 9.08
Yes 90.9

Art - Polling Netwk Trffc Abn IP
No 78.4
Yes 21.6

Art - Recur Proto SYN Traf
No 78.4
Yes 21.6

Art - Sequent Proto SYN T...
No 78.4
Yes 21.6

Art - Stat Anomalies Ntwk Tr
No 71.0
Yes 29.0

Art - DNS Port 53
No 85.0
Yes 15.0

Tech - Masquerading
No 76.2
Yes 23.8

Obs - GO Binaries
No 77.2
Yes 22.8

Obs - Bulky Files
No 95.1
Yes 4.91

Obs - Update dot e...
No 66.7
Yes 33.3

Obs - Stripped Executabl...
No 75.1
Yes 24.9

Tech - Service Stop
No 80.0
Yes 20.0
0.2 ± 0.4

Obs - Unauth RDP Traffic
No 80.8
Yes 19.2

Obs - Application Stop
No 78.6
Yes 21.4

Tech - Data Destruction
No 80.0
Yes 20.0
0.2 ± 0.4

Obs - Encrypted Fil...
No 80.8
Yes 19.2

Obs - Deleted Shadow Co...
No 80.8
Yes 19.2

Legend

Early-Mid-Late Stages
state0 100

Techniques
state0 100

Impacts
state0 100

Observables
state0 100

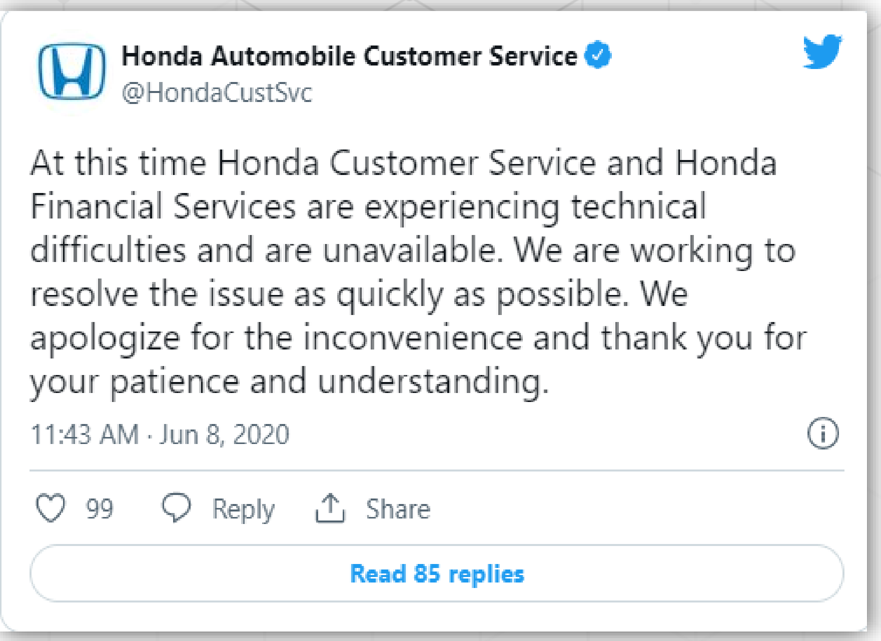
Tactic Categories
state0 100

Artifacts
state0 100

How is this applied to a CyOTE Precursor Analysis Report?

EKANS

- In the summer of 2020, three victim organizations in the manufacturing sector experienced interruptions to operations and loss of revenue due to ransomware targeting OT-specific application services.
- Impacts to Operational Technology:
  - Honda experienced a loss of production and revenue

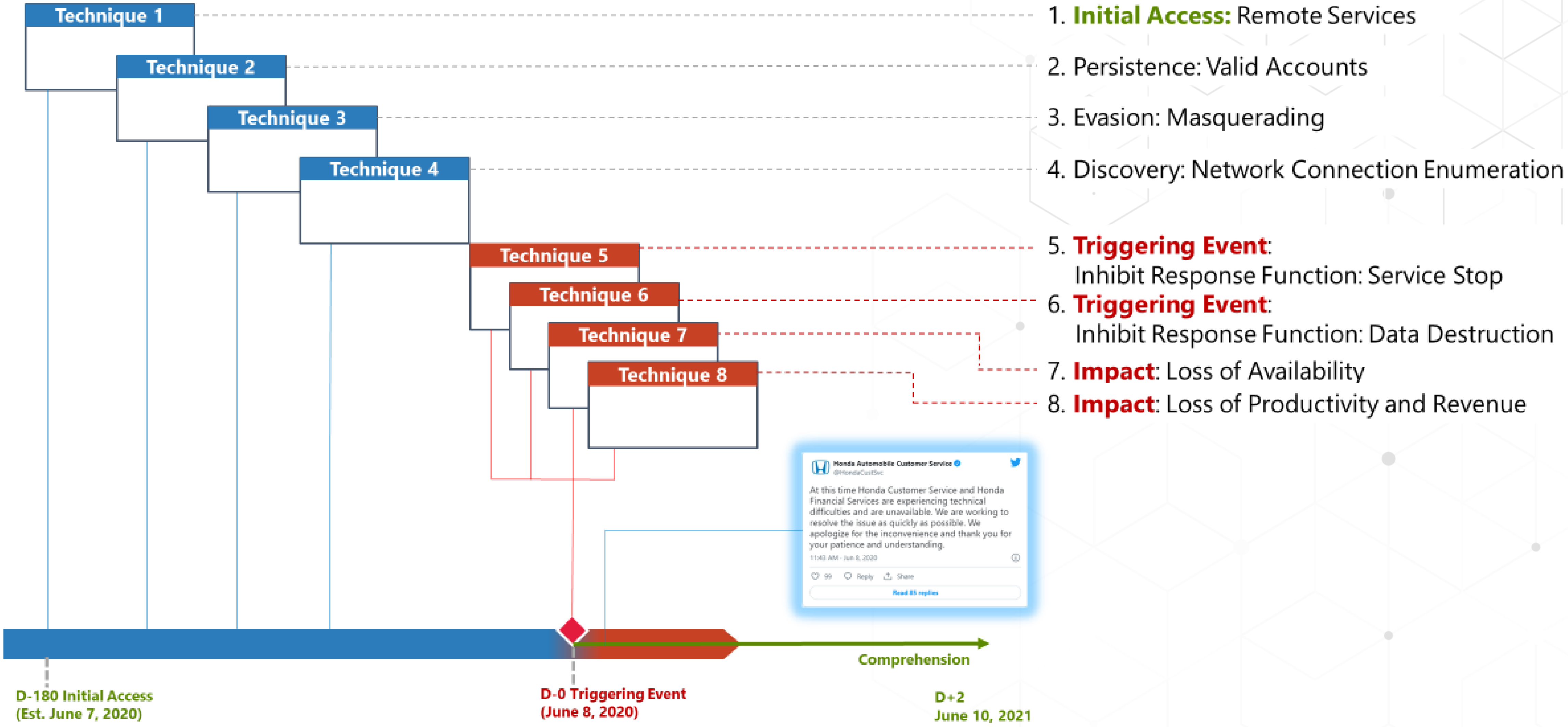


Honda Automobile Customer Service
@HondaCustSvc

At this time Honda Customer Service and Honda Financial Services are experiencing technical difficulties and are unavailable. We are working to resolve the issue as quickly as possible. We apologize for the inconvenience and thank you for your patience and understanding.

11:43 AM · Jun 8, 2020

EKANS Technique Timeline



1. **Initial Access:** Remote Services
2. Persistence: Valid Accounts
3. Evasion: Masquerading
4. Discovery: Network Connection Enumeration
5. **Triggering Event**: Inhibit Response Function: Service Stop
6. **Triggering Event**: Inhibit Response Function: Data Destruction
7. **Impact**: Loss of Availability
8. **Impact**: Loss of Productivity and Revenue

Honda Automobile Customer Service
@HondaCustSvc

At this time Honda Customer Service and Honda Financial Services are experiencing technical difficulties and are unavailable. We are working to resolve the issue as quickly as possible. We apologize for the inconvenience and thank you for your patience and understanding.

11:43 AM - Jun 8, 2020

99 Reply Share

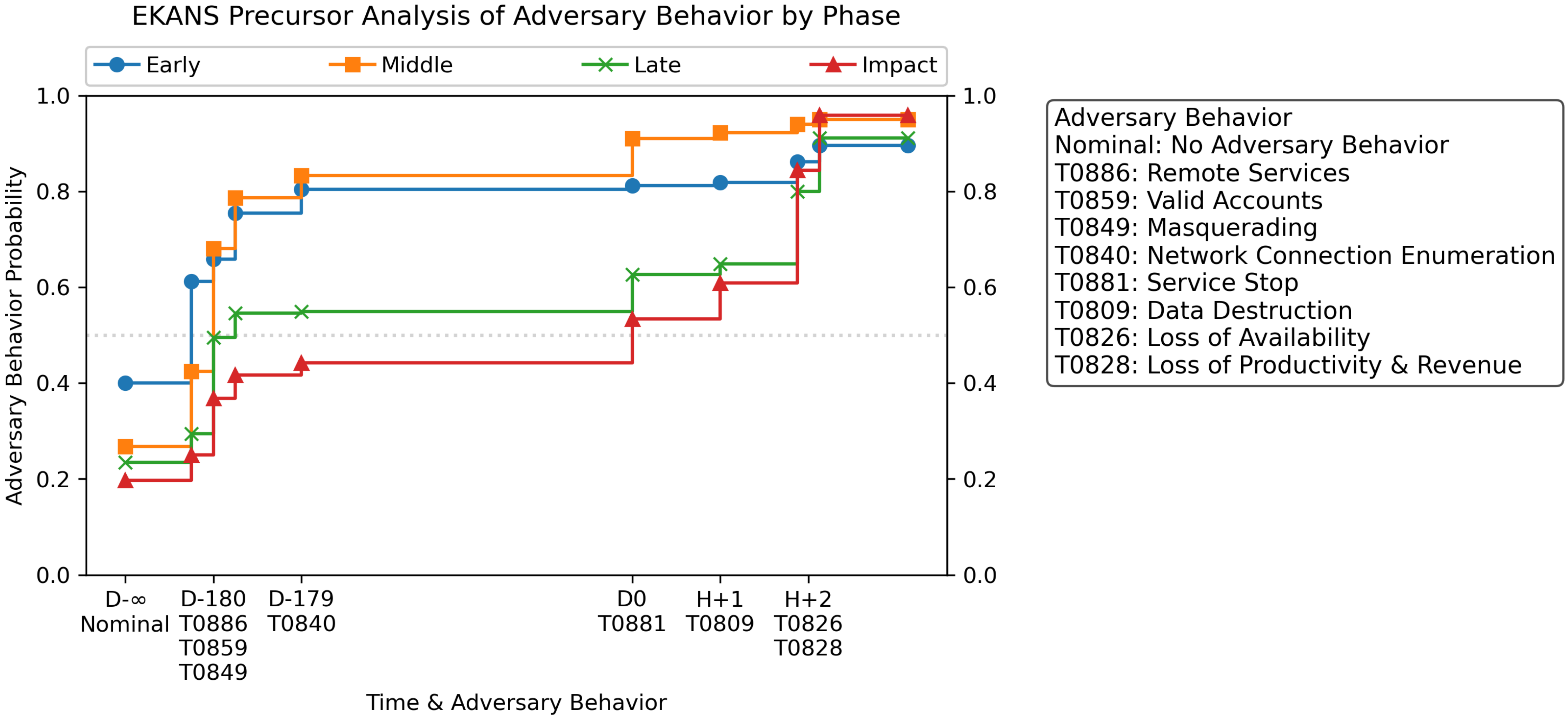
Read 85 replies

D-180 Initial Access
(Est. June 7, 2020)

D-0 Triggering Event
(June 8, 2020)

D+2
June 10, 2021

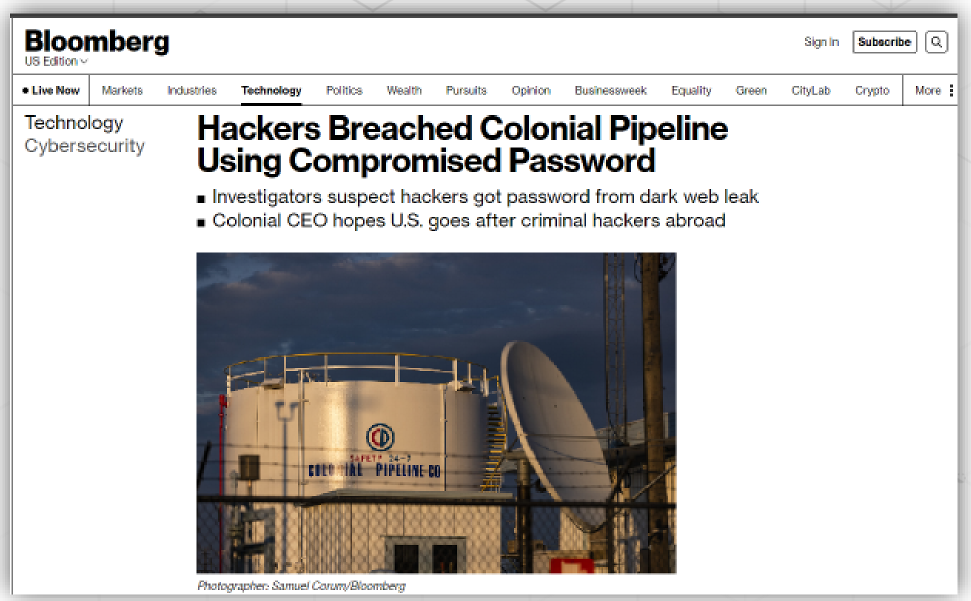
EKANS Probability of Adversary Behavior



Adversary Behavior
Nominal: No Adversary Behavior
T0886: Remote Services
T0859: Valid Accounts
T0849: Masquerading
T0840: Network Connection Enumeration
T0881: Service Stop
T0809: Data Destruction
T0826: Loss of Availability
T0828: Loss of Productivity & Revenue

Colonial Pipeline

- In the spring of 2021, the Colonial Pipeline experienced interruptions to operations and loss of revenue due to a ransomware attack on the enterprise network.
- Impacts to Operational Technology:
  - The largest pipeline in the United States was shut down for five days and $4.4 million was paid in ransom.



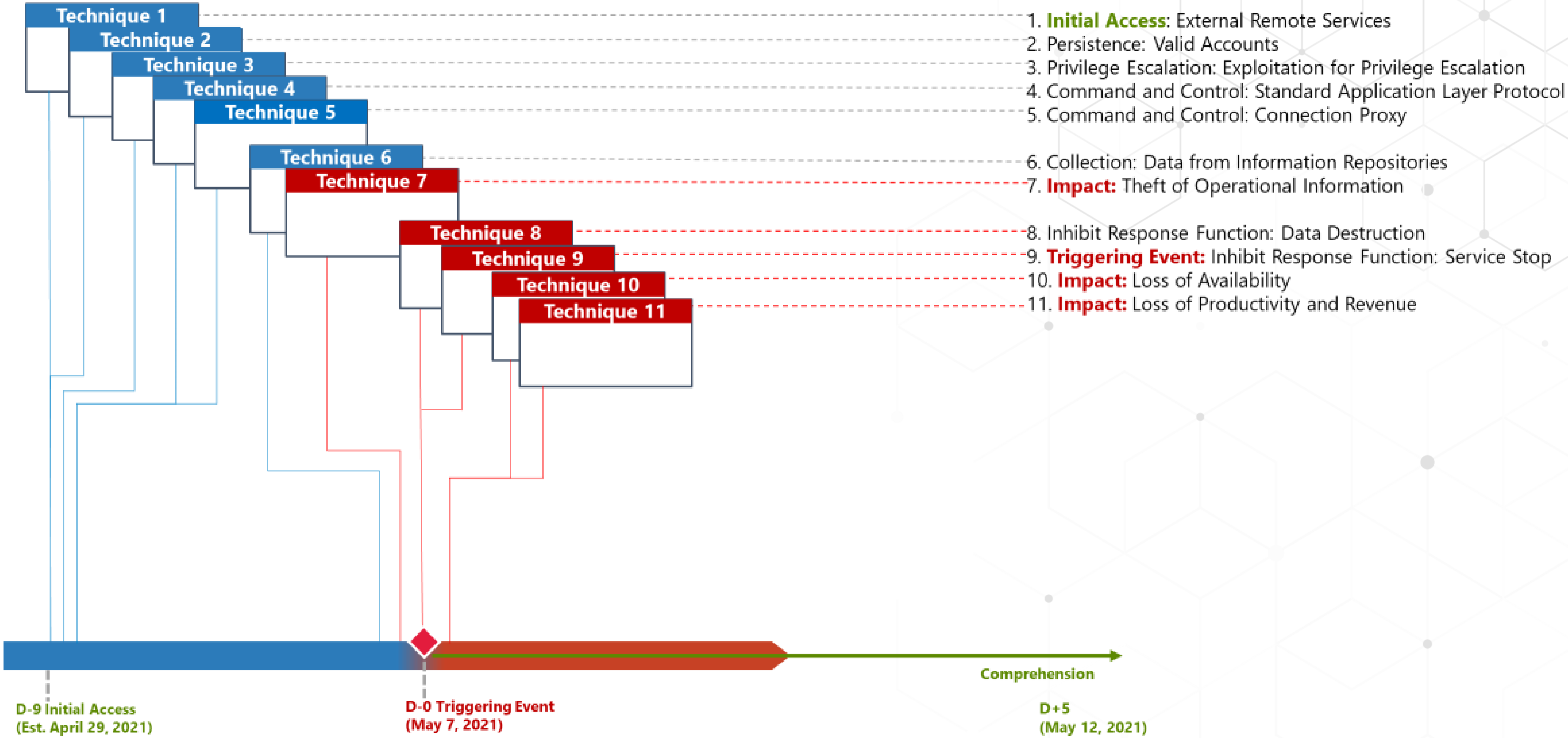
Technology
Cybersecurity

Hackers Breached Colonial Pipeline Using Compromised Password

- Investigators suspect hackers got password from dark web leak
- Colonial CEO hopes U.S. goes after criminal hackers abroad

Photographer: Samuel Corum/Bloomberg

Colonial Pipeline Attack Timeline



1. **Initial Access**: External Remote Services
2. Persistence: Valid Accounts
3. Privilege Escalation: Exploitation for Privilege Escalation
4. Command and Control: Standard Application Layer Protocol
5. Command and Control: Connection Proxy

6. Collection: Data from Information Repositories
7. **Impact:** Theft of Operational Information

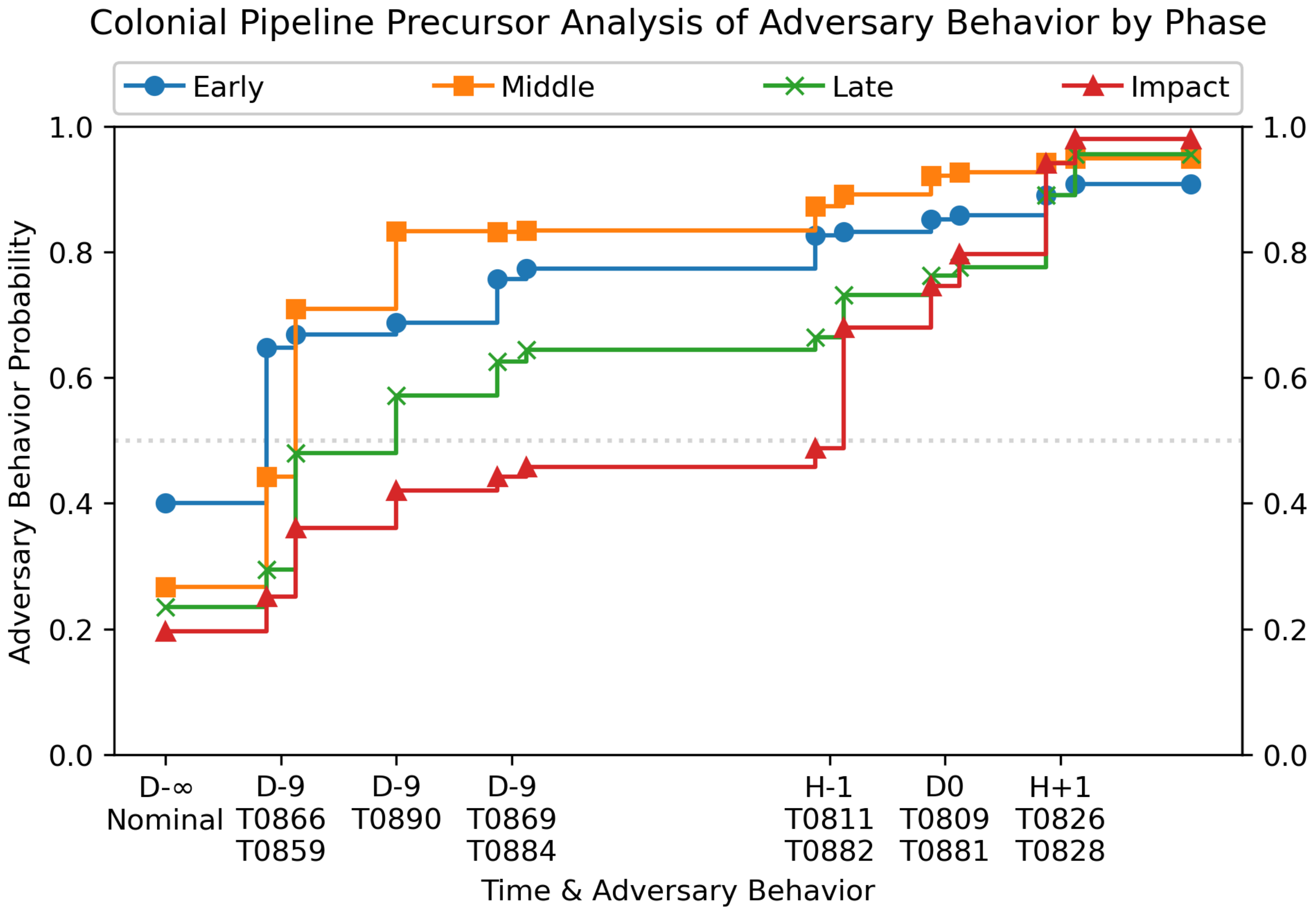
8. Inhibit Response Function: Data Destruction
9. **Triggering Event:** Inhibit Response Function: Service Stop
10. **Impact:** Loss of Availability
11. **Impact:** Loss of Productivity and Revenue

D-9 Initial Access
(Est. April 29, 2021)

D-0 Triggering Event
(May 7, 2021)

D+5
(May 12, 2021)

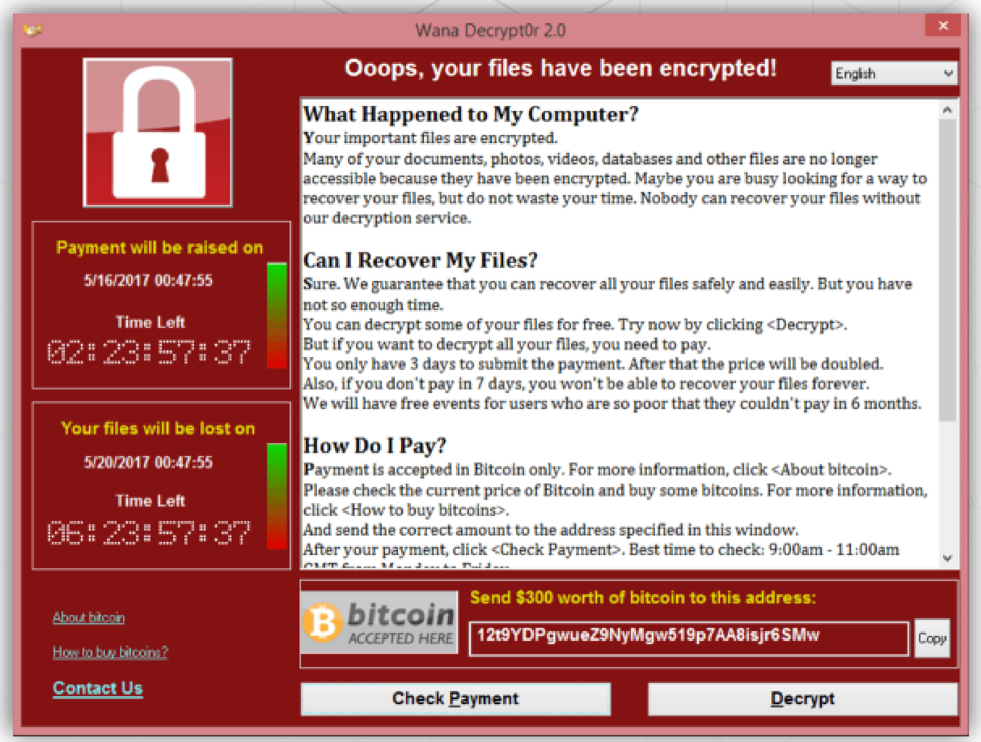
Colonial Pipeline Probability of Adversary Behavior



Adversary Behavior
Nominal: No Adversary Behavior
T0866: Exploitation of Remote Services
T0859: Valid Accounts
T0890: Exploitation for Privilege Escalation
T0869: Standard Application Layer Protocol
T0884: Connection Proxy
T0811: Data from Information Repositories
T0882: Theft of Operational Information
T0809: Data Destruction
T0881: Service Stop
T0826: Loss of Availability
T0828: Loss of Productivity & Revenue

WannaCry

- In the spring of 2017, Renault-Nissan manufacturing plants experienced interruptions to operations and loss of revenue due to WannaCry ransomware leveraging multiple exploits.
- Impacts to Operational Technology:
  - Renault-Nissan shut down five manufacturing plants for three days



Ooops, your files have been encrypted!

Payment will be raised on

5/16/2017 00:47:55

Time Left

02:23:57:37

Your files will be lost on

5/20/2017 00:47:55

Time Left

06:23:57:37

What Happened to My Computer?

Your important files are encrypted.

Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.

Can I Recover My Files?

Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time.

You can decrypt some of your files for free. Try now by clicking <Decrypt>.

But if you want to decrypt all your files, you need to pay.

You only have 3 days to submit the payment. After that the price will be doubled.

Also, if you don't pay in 7 days, you won't be able to recover your files forever.

We will have free events for users who are so poor that they couldn't pay in 6 months.

How Do I Pay?

Payment is accepted in Bitcoin only. For more information, click <About bitcoin>.

Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>.

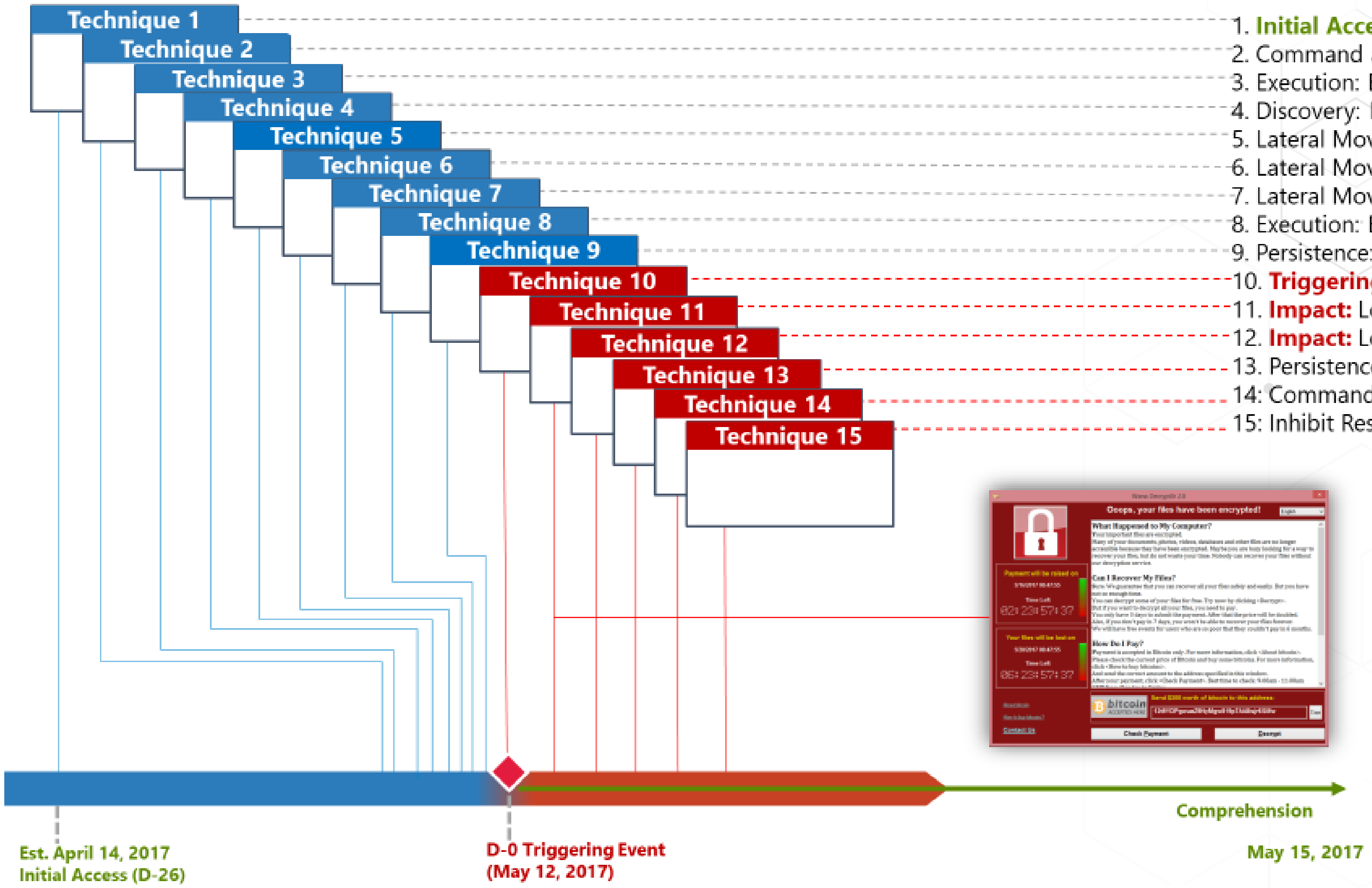
And send the correct amount to the address specified in this window.

After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am

Send $300 worth of bitcoin to this address:

12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw

WannaCry Technique Timeline



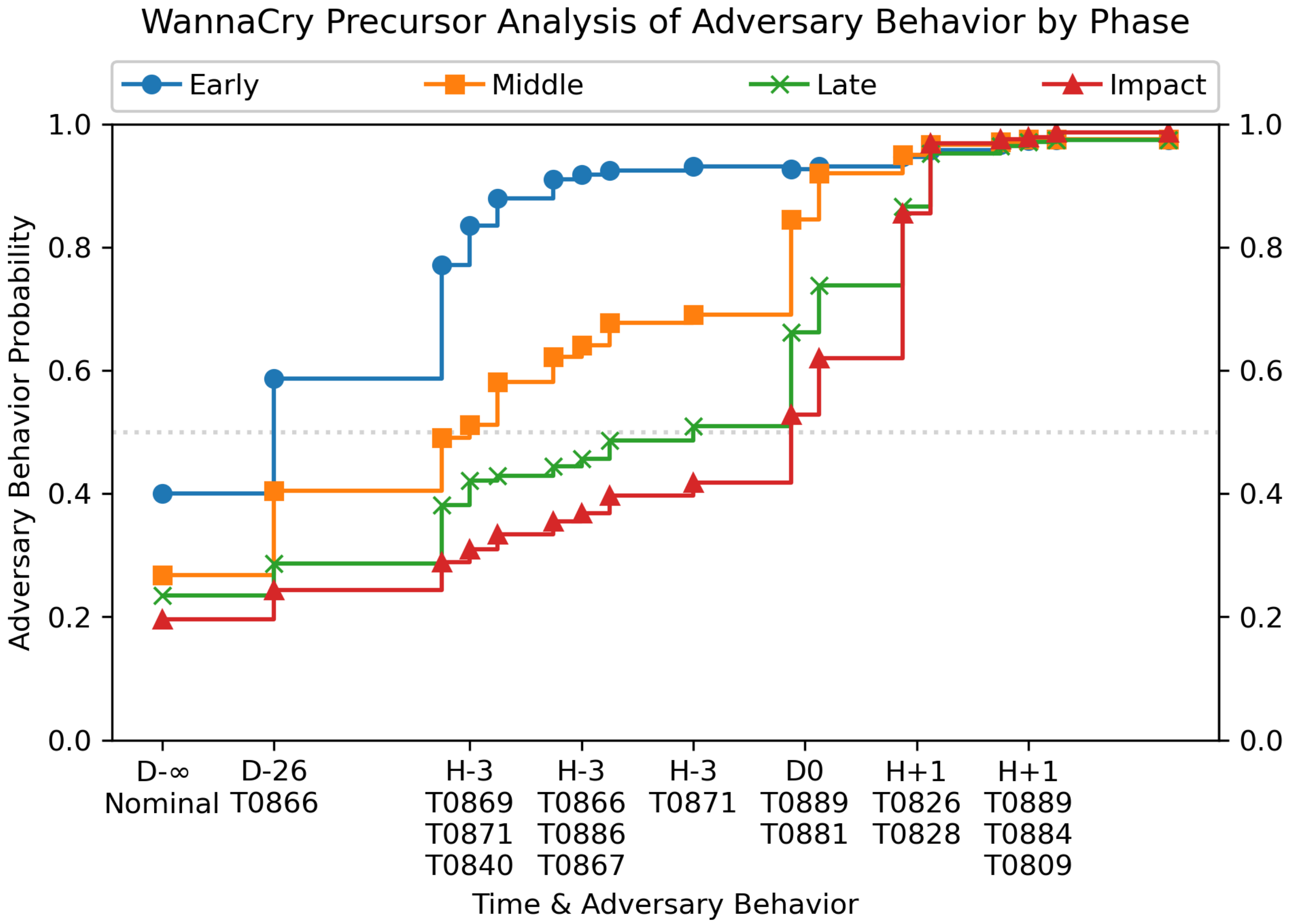
Est. April 14, 2017
Initial Access (D-26)

D-0 Triggering Event
(May 12, 2017)

May 15, 2017

1. **Initial Access**: Exploitation of Remote Services
2. Command and Control: Standard Application Layer Protocol
3. Execution: Execution through API
4. Discovery: Network Connection Enumeration
5. Lateral Movement: Exploitation of Remote Services
6. Lateral Movement: Remote Services
7. Lateral Movement: Lateral Tool Transfer
8. Execution: Execution through API
9. Persistence: Modify Program
10. **Triggering Event:** Inhibit Response Function: Service Stop
11. **Impact:** Loss of Availability
12. **Impact:** Loss of Productivity and Revenue
13. Persistence: Modify Program
14: Command and Control: Connection Proxy
15: Inhibit Response Function: Data Destruction

WannaCry Probability of Adversary Behavior

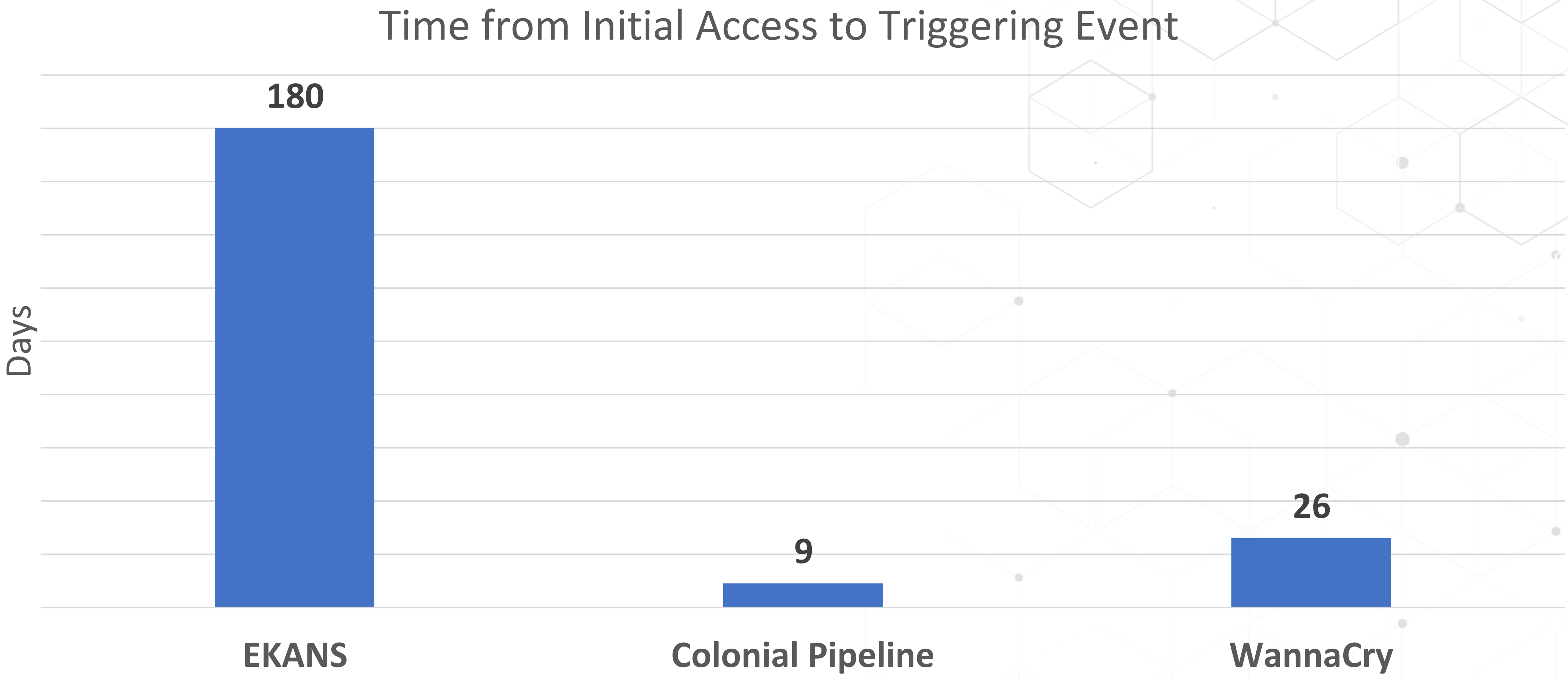


WannaCry Precursor Analysis of Adversary Behavior by Phase

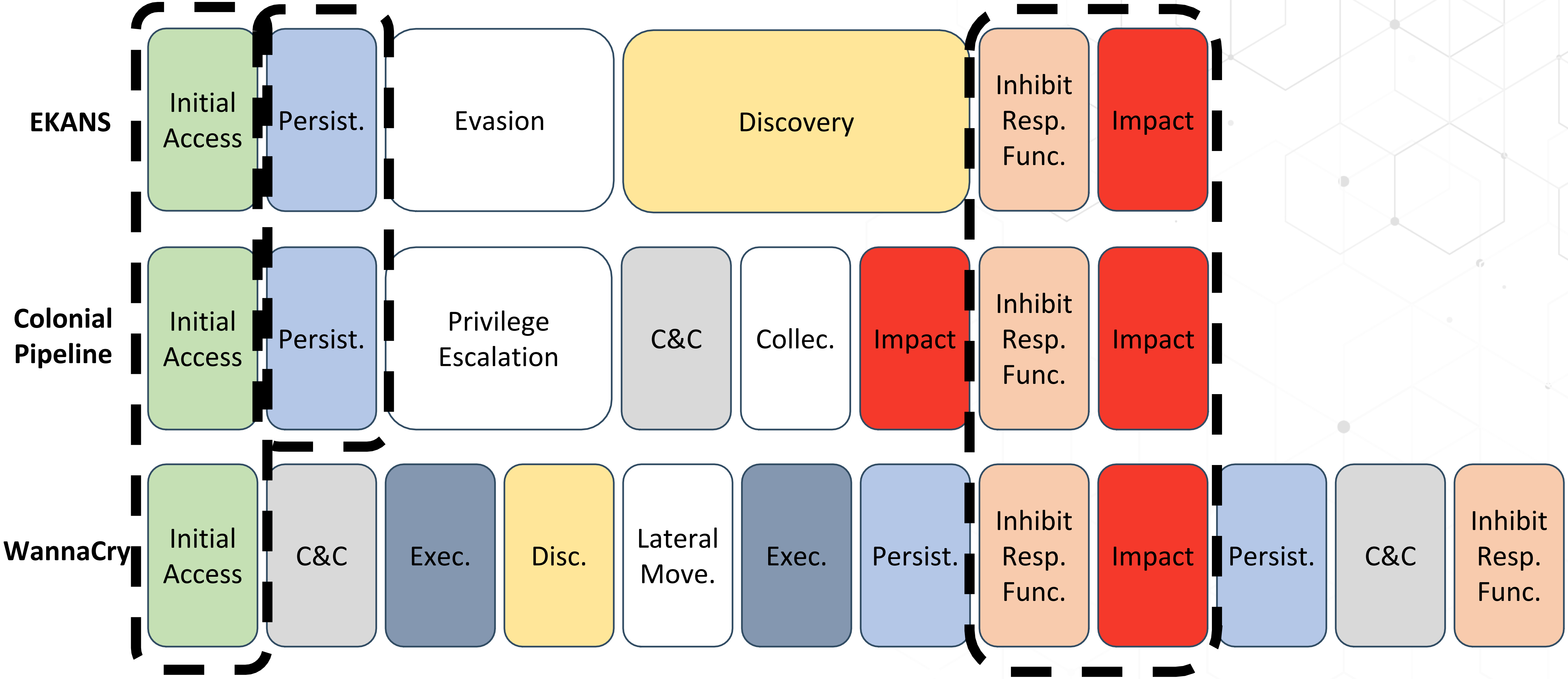
Adversary Behavior
Nominal: No Adversary Behavior
T0866: Exploitation of Remote Services
T0869: Standard Application Layer Protocol
T0871: Execution through API
T0840: Network Connection Enumeration
T0866: Exploitation of Remote Services
T0886: Remote Services
T0867: Lateral Tool Transfer
T0871: Execution through API
T0889: Modify Program
T0881: Service Stop
T0826: Loss of Availability
T0828: Loss of Productivity & Revenue
T0889: Modify Program
T0884: Connection Proxy
T0809: Data Destruction

What are the differences between the reports?

Dwell time varied significantly across cases



The sequence of intermediate tactics varied significantly

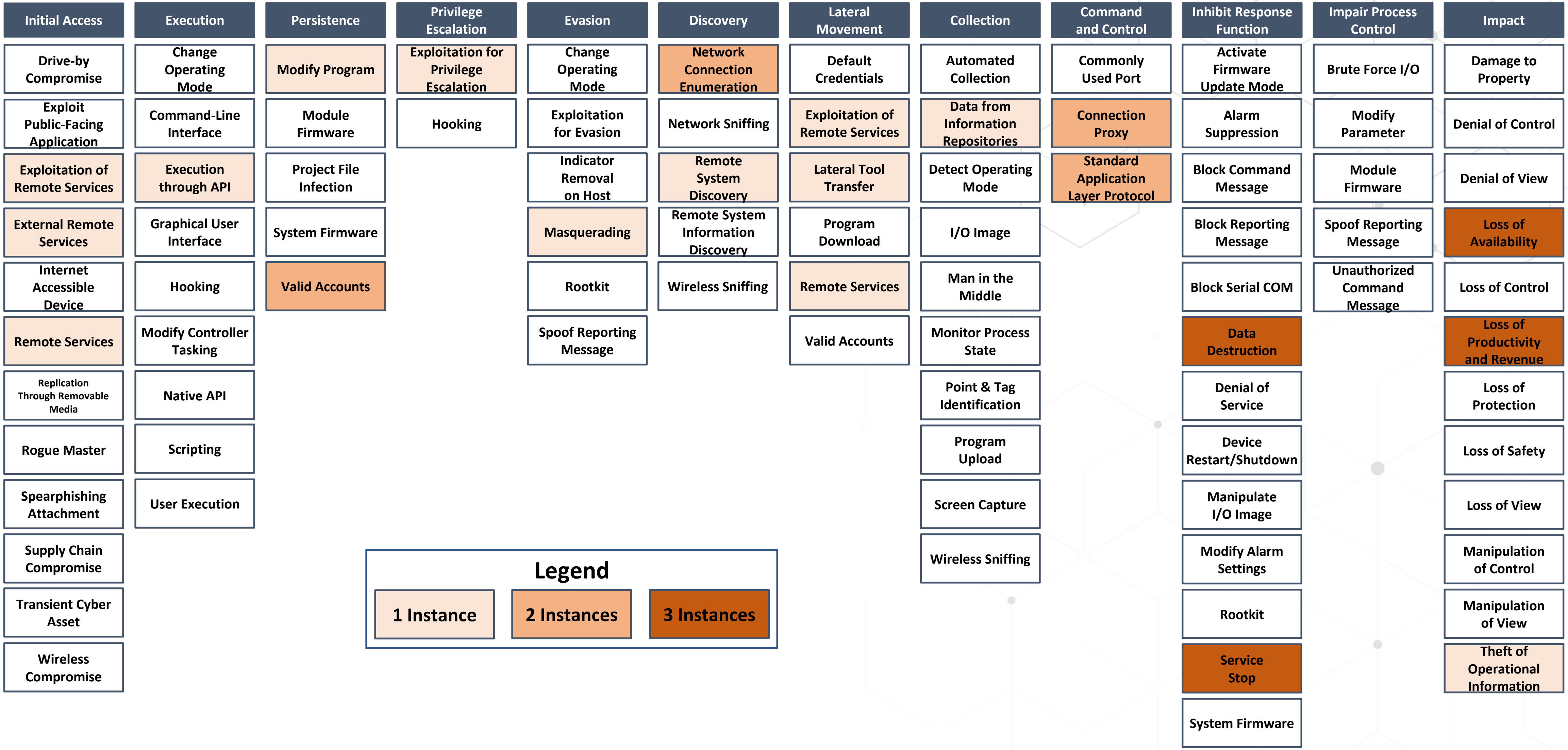


EKANS: Initial Access, Persist., Evasion, Discovery, Inhibit Resp. Func., Impact

Colonial Pipeline: Initial Access, Persist., Privilege Escalation, C&C, Collec., Impact, Inhibit Resp. Func., Impact

WannaCry: Initial Access, C&C, Exec., Disc., Lateral Move., Exec., Persist., Inhibit Resp. Func., Impact, Persist., C&C, Inhibit Resp. Func.

MITRE ATT&CK® for ICS

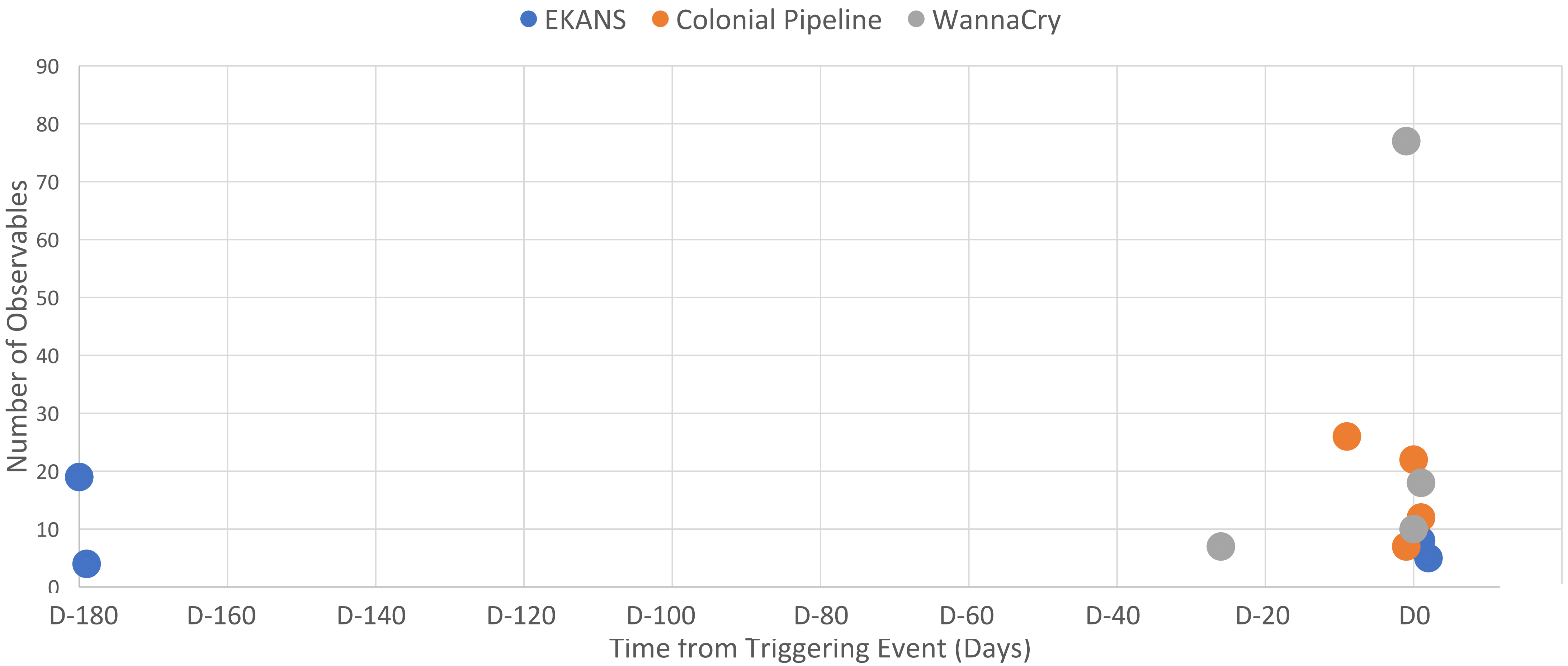


Initial Access	Execution	Persistence	Privilege Escalation	Evasion	Discovery	Lateral Movement	Collection	Command and Control	Inhibit Response Function	Impair Process Control	Impact
Drive-by Compromise	Change Operating Mode	Modify Program	Exploitation for Privilege Escalation	Change Operating Mode	Network Connection Enumeration	Default Credentials	Automated Collection	Commonly Used Port	Activate Firmware Update Mode	Brute Force I/O	Damage to Property
Exploit Public-Facing Application	Command-Line Interface	Module Firmware	Hooking	Exploitation for Evasion	Network Sniffing	Exploitation of Remote Services	Data from Information Repositories	Connection Proxy	Alarm Suppression	Modify Parameter	Denial of Control
Exploitation of Remote Services	Execution through API	Project File Infection		Indicator Removal on Host	Remote System Discovery	Lateral Tool Transfer	Detect Operating Mode	Standard Application Layer Protocol	Block Command Message	Module Firmware	Denial of View
External Remote Services	Graphical User Interface	System Firmware		Masquerading	Remote System Information Discovery	Program Download	I/O Image		Block Reporting Message	Spoof Reporting Message	Loss of Availability
Internet Accessible Device	Hooking	Valid Accounts		Rootkit	Wireless Sniffing	Remote Services	Man in the Middle		Block Serial COM	Unauthorized Command Message	Loss of Control
Remote Services	Modify Controller Tasking			Spoof Reporting Message		Valid Accounts	Monitor Process State		Data Destruction		Loss of Productivity and Revenue
Replication Through Removable Media	Native API						Point & Tag Identification		Denial of Service		Loss of Protection
Rogue Master	Scripting						Program Upload		Device Restart/Shutdown		Loss of Safety
Spearphishing Attachment	User Execution						Screen Capture		Manipulate I/O Image		Loss of View
Supply Chain Compromise							Wireless Sniffing		Modify Alarm Settings		Manipulation of Control
Transient Cyber Asset									Rootkit		Manipulation of View
Wireless Compromise									Service Stop		Theft of Operational Information
									System Firmware		

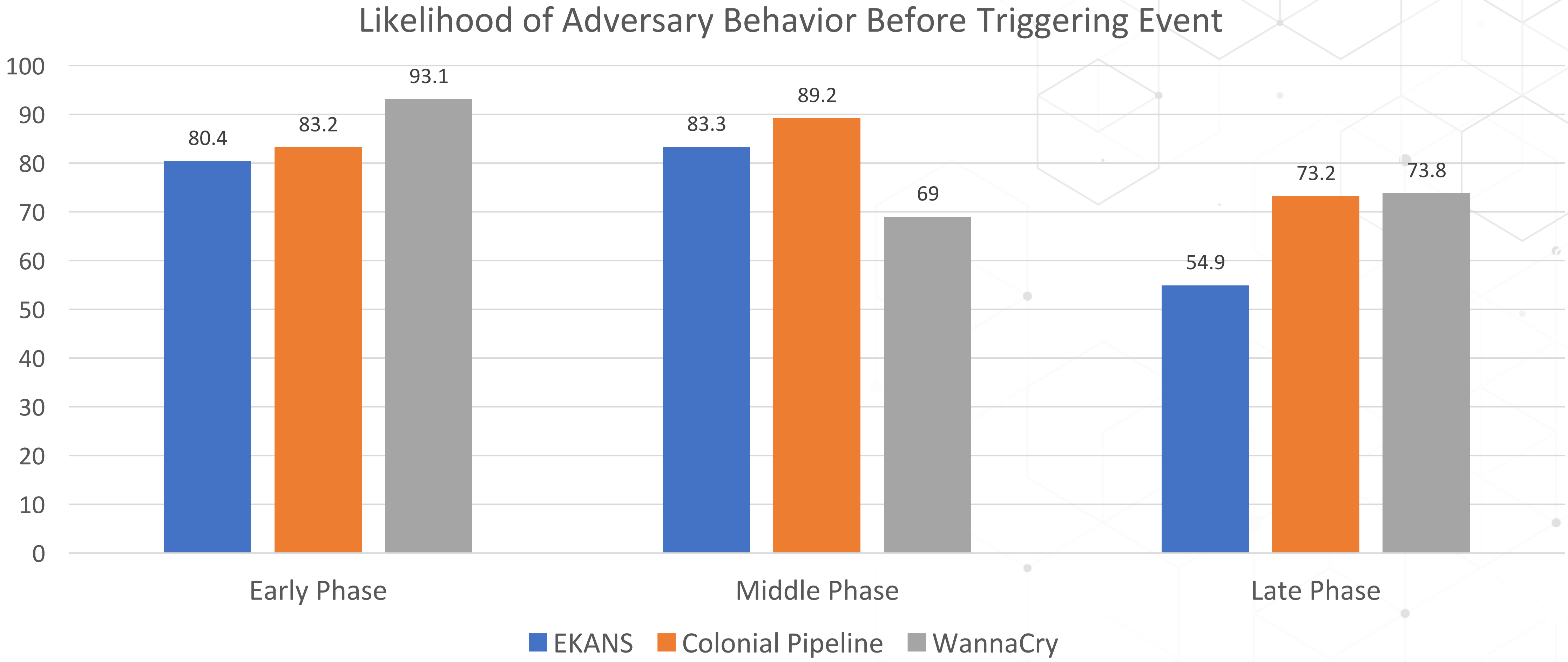
Legend

1 Instance | 2 Instances | 3 Instances

The occurrence of observables varied significantly



Precursor evidence strongly indicated adversary behavior



Take-Aways

- Demonstrates how observers value cyber-events and estimates likelihood of adversarial behavior
- Demonstrates value of cumulative precursor evidence
- Provides justification for investigation of related events
- Demonstrates diagnosticity of the evidence
- Enables improvement of observers’ belief systems
- Training tool for improving human perception & comprehension of observables
- Enables future meta-analysis of case studies

For questions contact:

Gabriel Weaver, CyOTE Precursor Analysis Program Analyst, Gabriel.Weaver@inl.gov

Lee Maccarone, Lead CyOTE Precursor Analysis Program Risk Analyst, lmaccar@sandia.gov

@DOE_CESER

linkedin.com/company/office-of-cybersecurity-energy-security-and-emergency-response

energy.gov/CESER

This presentation was prepared by Idaho National Laboratory (INL) under an agreement with and funded by the U.S. Department of Energy. INL is a U.S. Department of Energy National Laboratory operated by Battelle Energy Alliance, LLC.

Sandia National Laboratories is a multimission laboratory managed and operated by National Technology & Engineering Solutions of Sandia, LLC, a wholly owned subsidiary of Honeywell International Inc., for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-NA0003525.